



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /aba	8250
7380 7590 03/29/2007 SMART & BIGGAR P.O. BOX 2999, STATION D 900-55 METCALFE STREET OTTAWA, ON K1P5Y6 CANADA			EXAMINER AGWUMEZIE, CHARLES C	
			ART UNIT 3621	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		03/29/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/702,540

Applicant(s)

SO, VINCENT

Examiner

Charlie C. Agwumezie

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 January 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 and 34-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 and 34-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>11/7/03</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims status

1. Claims 24-33 are cancelled. Claims 35, and 37 are amended. Claims 1-23 and 34-43 are pending in this application per the response to office action filed on January 24, 2007.

Response to Arguments

2. Applicant's arguments filed January 24, 2007 have been fully considered but they are not persuasive.

With respect to claim 1, 15 and 38, Applicant argues that Peterka et al fails to teach or fairly suggest that decryption keys are delivered to a customer processing platform "in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time" as recited in claims 1, 15 and 38.

In response, Examiner respectfully disagrees with Applicant's characterization of Peterka's invention and submits that Peterka clearly discloses that decryption keys are delivered to a customer processing platform "in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time" as recited in claims 1, 15 and 38 and as shown in the rejections below. In addition to PSks, Peterka et al is replete with scenarios where content keys for each segment are provided to the customer (fig. 7; 0093).

As per claims 35, 36 and 37, Applicant's arguments/amendments with respect to claims 35, 36 and 37 have been considered but are moot in view of the new ground(s) of rejection. Accordingly, the Mourad reference is hereby withdrawn.

As per claim 2, Applicant alleges that Examiner applied hindsight analysis in that both Peterka et al and Stirling et al fails to teach or fairly suggest encrypting a plurality of sections of data content with corresponding plurality of encryption keys and distributing decryption keys corresponding to the decryption keys to the processing platform of a consumer in a manner such that the consumer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time" as recited in independent claims 1. Applicant further argues that Examiner is incorrect in equating the destroying of decryption key when it is no longer needed by the decryption as taught by Stirling et al with the destroying of a first decryption key at a customer processing platform.

In response, Examiner incorporates the discussion above in claim 1 as if fully rewritten here. Furthermore, in response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). According to Applicant's specification, after the current section is finished (i.e.

Art Unit: 3621

current decryption), the current key is destroyed and the next section is decrypted. In other words the first key is destroyed after the first key is used and is no longer needed. The key is destroyed because the key has been used to complete the playback of the encrypted section and therefore no longer needed. Accordingly the combination of the prior art references of record is proper in all respects and the rejection must be maintained.

As per claims 3-6, Applicant argues that the argument advanced in response to claim 2 is applicable to claims 3-6. Thus claims 3-6 are distinguishable over Peterka et al and Stirling alone or in combination and for at least the reasons for claim 2.

In response, Examiner respectfully disagrees and submits that claims 3-6 are not distinguishable over Peterka et al in view of Stirling et al reference.

As per claim 7, Applicant argues that the billing in Peterka et al is completely different from the claimed billing in the current application.

In response, Examiner respectfully disagrees and submits that no distinction can be established between the two billings as claimed.

As per claims 8 and 9, Applicant argues depends on claim 1 which Applicant alleges is distinguishable over the teachings of Peterka et al and therefore claims 8 and 9 are distinguishable over the teachings of Peterka et al.

In response, Examiner respectfully disagrees and asserts that neither claim 1 nor the dependent claims 8 and 9 are distinguishable over the teachings of Peterka et al.

As per claim 10, Applicant argues that Peterka et al fails to teach or fairly suggest that the encryption keys used to encrypt the section of data content i.e. the

Art Unit: 3621

content keys (CK) are generated "using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing-specific keys."

In response, Examiner respectfully disagrees with Applicant characterization of Peterka et al and submits that Peterka clearly discloses a method wherein the key is unique per viewer. Incidentally each client on a network must have a unique identifier or a unique network name (0097; 0110; 0114). The unique keys of Peterka et al is associated with the content key, service key, program key or program segment key. Thus Peterka clearly teaches all of the claimed limitations of claim 10.

As per claim 11, Applicant argues that Peterka et al fails to teach or fairly suggest that each encryption key is generated using an identifier associated with a customer processing platform and respective key generation seed value.

In response, Examiner respectfully disagrees and submits that Peterka et al clearly discloses that each encryption key is generated using an identifier associated with a customer processing platform and respective key generation seed value. A decryption key seed value according to Applicant's specification is the decryption key seed value that is combined with or transformed using such a unique identifier to generate the decryption keys. A customer unique key is specific to each viewer according to Peterka. How does one generate a unique key without anything unique about the client? How does the server send a unicast message to a client if it does not have a unique address to the particular client?

Art Unit: 3621

As per **claim 12**, Applicant argues that Peterka et al fails to teach or fairly suggest that delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values.

In response, Applicant is directed to see response to claim 11 above.

As per **claim 13**, Applicant argues depends on claim 1 which Applicant alleges is distinguishable over the teachings of Peterka et al and therefore claim 13 is distinguishable over the teachings of Peterka et al.

In response, Examiner respectfully disagrees and asserts that neither claim 1 nor the dependent claim 13 is distinguishable over the teachings of Peterka et al.

As per **claims 16 and 21**, Applicant submits that the arguments presented with respect to claim 2 is also applicable to the rejections of claim 16 and 21.

In response, Applicant is directed to the discussions with respect to claim 2 above as the arguments with respect to claim 2 above is also applicable to claims 16 and 21.

As per **claim 17**, Applicant argues that Stirling does not teach or fairly suggest "destroying decrypted data content at the customer processing platform after completing playback of the encrypted section.

In response, Stirling clearly discloses "destroying decrypted data content at the customer processing platform after completing playback of the encrypted section (when it is no longer needed) as discussed in claim 2 above.

As per claims 18 and 19, Applicant argues depends on claim 16 which Applicant alleges is distinguishable over the teachings of Peterka et al and therefore claims 18 and 19 are distinguishable over the teachings of Peterka et al.

In response, Examiner respectfully disagrees and asserts that neither claim 16 nor the dependent claims 18 and 19 are distinguishable over the teachings of Peterka et al.

As per claim 22, Applicant argues that encrypting a content key for the purposes of multicast transmission is completely different than encrypting the plurality of sections of data content with plurality of customer processing platform specific keys which are determined based on an IP address of the customer processing platform.

In response, Examiner respectfully disagrees with the Applicant's characterization and submits that Peterka et al clearly discloses that a unique key is employed for the purposes of the multicast/unicast transmission. Peterka et al further directed us to assume that for the purposes of multicast addressing, that multicast IP addressing allocation and assignment is transparent to any internet protocol (0038). Thus it is clear that one way to archive unique transmission and traceability is to use the IP address of the client, which is always unique to each client.

As per claim 23, Applicant argues depends on claim 16 which Applicant alleges is distinguishable over the teachings of Peterka et al and therefore claim 23 are distinguishable over the teachings of Peterka et al.

In response, Examiner respectfully disagrees and asserts that neither claim 16 nor the dependent claim 23 is distinguishable over the teachings of Peterka et al.

As per **claim 39**, Applicant submits that the arguments presented with respect to claim 2 is also applicable to the rejections of claim 39.

In response, Applicant is directed to the discussions with respect to claim 2 above as the arguments with respect to claim 2 above is also applicable to claim 39.

As per **claim 40**, Applicant's argument with respect to claim 40 have been considered but are moot in view of the new ground(s) of rejection.

However Applicant argues that Peterka et al and Stirling et al, alone or in combination, fails to teach or fairly suggest a data content server configured to "transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content" and a data content download controller configured to "generate permission request when the downloaded data content is to be used."

In response, Examiner respectfully disagrees and submits that Peterka et al and Stirling et al alone or in combination does disclose a data content server configured to "transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content" and a data content download controller configured to "generate permission request when the downloaded data content is to be used" as recited in claim 40 and as shown in the rejections.

As per **claims 41 and 42**, Applicant argues depends on claim 40 which Applicant alleges is distinguishable over the teachings of Peterka et al and therefore claims 41 and 42 are distinguishable over the teachings of Peterka et al.

Art Unit: 3621

In response, Examiner respectfully disagrees and asserts that neither claim 40 nor the dependent claims 41 and 42 are distinguishable over the teachings of Peterka et al in combination of Stirling et al as shown in the rejections.

As per claim 14, Applicant argues depends on claim 1 which Applicant alleges is distinguishable over the teachings of Peterka et al and therefore claim 14 is distinguishable over the teachings of Peterka et al.

In response, Examiner respectfully disagrees and asserts that neither claim 1 nor the dependent claim 14 is distinguishable over the teachings of Peterka et al.

As per claims 20 and 43, Applicant argues depends on claims 16 and 40 respectively and that Peterka et al and Stirling et al fails to teach or fairly suggest key limitations of claims 20 and 43. Applicant also argues that Ginter et al fails to teach or fairly suggest key limitations of claims 20 and 43 and therefore claims 20 and 43 are distinguishable over the teachings of Peterka et al, Stirlings et al and Ginter et al both alone or in combination.

In response, Examiner respectfully disagrees and submits that claim 20 and 43 are not distinguishable from the teaching of the references of records are shown in the rejections.

As per claim 34, Applicant argues that Negawa's deletion or destruction of the decryption key is completely different from the Applicant's "for each subsequent portion of the encrypted data: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data; causing a key for

Art Unit: 3621

a preceding portion of the encrypted data to be deleted from the customer data content processing device.

In response, Examiner respectfully disagrees with the Applicant characterization and submits that Peterka et al in combination of Negawa does disclose all the limitations of claim 34 as shown in the rejections. Furthermore by incorporating Negawa with Peterka et al does not in any way render Peterka et al unsuitable for its intended purpose as alleged by the Applicant. Thus claim 34 is properly rejected as shown in the rejections below.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 7-13, 15, 35-37, 38 and 40-42, are rejected under 35 U.S.C. 102(e) as

being anticipated by Peterka et al U.S. Patent Application Publication No.

2002/0170053 A1.

As per **claims 1, 15 and 38**, Peterka et al discloses a method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections (0080; 0082; 0101);

delivering the plurality of encrypted sections to the customer processing platform (fig. 8; 0080; 0082); and

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time (see fig. 7; 0080; 0082; 0102; 0093; ...client has possession of program segment key and next the key...as well as content key 0, 1, 2, 3, 4,).

As per **claim 7**, Peterka et al further discloses the method further comprising:

billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform (figs. 8 and 9).

As per **claim 8**, Peterka et al further discloses the method, wherein the data content is video content or music content, and wherein use of the data content at the

Art Unit: 3621

customer processing platform comprises decryption and playback of the data content (0033; 0080; 0082).

As per claim 9, Peterka et al further discloses the method, wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key (0080; 0082; 0117).

As per claim 10, Peterka et al further discloses the method, further comprising:
generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys (0097; 0114; 0124).

As per claim 11, Peterka et al further discloses the method, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value (0097; 0114; 0124; claim 23).

As per claim 12, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values (0097; 0114; 0124; claim 23).

As per claim 13, Peterka et al further discloses the method, further comprising:
generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform (0097; 0114; 0124; claim 23),

wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values (0097; 0114; 0124; claim 23).

As per claims 35, and 37, Peterka et al discloses a computer readable medium storing software code executable by a processing platform, the software code comprising:

first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system (fig. 7; 0080; 0082; 0101); and
second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decrypting keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any

Art Unit: 3621

time (see fig. 7; 0080; 0082; 0102; ...client has possession of program segment key and next the key...).

As per claim 36, Peterka et al further discloses the computer readable medium, wherein the second software code obtains further permissions from the data content service provider system to continue using the data content (fig. 15; ...permit the client who received the second key to decrypt the encrypted program content...).

As per claim 40, Peterka et al discloses a data content distribution system comprising:

a data content server configured to receive download requests and permission requests for data content, to encrypt a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and to transmit the encrypted sections of the data content in response to a received download request for the data content, and to transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content (figs. 1, 3, 8, 9 and 15); and

a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the

Art Unit: 3621

corresponding one of the plurality of decryption keys (fig. 1, 7 and 81; 0080; 0082; ...receive a purchase request from a purchasing client for the program content...as well as content keys 0, 1, 2, 3, 4...).

As per **claim 41**, Peterka et al further discloses the system, comprising a data network connecting the data content server and the data content download controller (fig. 1).

As per **claim 42**, Peterka et al further discloses the system, further comprising a plurality of data content download controllers connected to the data network (fig. 1).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2-6, 16-19, 21-23, and 39, are rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Stirling et al U.S. patent Application Publication No. 2003/0223583 A1.

As per claim 2, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a first key of the plurality of decryption keys for a first encrypted section of the plurality of encrypted sections (figs. 3 and 6; 0080; 0082);

delivering to the customer processing platform a second key of the plurality of decryption keys for a second encrypted section of the plurality of encrypted sections (0007).

What Peterka et al does not explicitly teach is

causing the first key to be destroyed at the customer processing platform.

Stirling et al discloses the method of delivering data content comprising causing the first key to be destroyed at the customer processing platform (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the first key to be destroyed at the customer processing platform in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

As per claim 3, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a current key of the plurality of decryption keys for a current encrypted section of the plurality of encrypted sections to be processed at the customer processing platform (0080; 0082);

delivering to the customer processing platform a next key of the plurality of decryption keys for a next encrypted section of the plurality of encrypted sections to be subsequently processed at the customer processing platform upon completion of processing of the current encrypted section (0080; 0082; 0102; ...client has possession of program segment key and next key...).

What Peterka et al does not explicitly teach is

causing the first key to be destroyed at the customer processing platform.

Stirling et al discloses method of delivering data content comprising causing the first key to be destroyed at the customer processing platform (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the first key to be destroyed at the customer processing platform in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

As per **claim 4**, Peterka et al further discloses the method, wherein delivering to the customer processing platform a next key of the plurality of decryption keys (0080; 0082) and

What Peterka does not explicitly teach is causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed.

Stirling et al discloses causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

As per claim 5, Peterka et al discloses the method, wherein the current encrypted section is a first one of the plurality of encrypted sections (0080; 0082), and wherein delivering to the customer processing platform a next key of the plurality of decryption keys (0080; 0082).

What Peterka et al does not explicitly teach is causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section.

Art Unit: 3621

Stirling et al discloses causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering data content comprising causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

As per claim 6, Peterka et al further discloses the method, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

providing key control software to the customer processing platform, the key control software being adapted to: receive a decryption key for one of the plurality of encrypted sections (0080; 0082; 0117; 0118);

complete decryption of the one section (0080; 0082).

What Peterka et al does not explicitly teach is

destroy the decryption key.

Stirling et al discloses a method comprising destroy the decryption key (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the

Art Unit: 3621

method of destroy the decryption key in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

As per claims 16 and 21, Peterka et al discloses a method of receiving and controlling playback of data content at a customer processing platform, comprising:
receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key (fig. 1; 0080; 0082);

and for each encrypted section:
receiving a decryption key in respect of the encrypted section (0080; 0082);
decrypting and playing back the encrypted section using the decryption key (0033; 0080; 0082).

What Peterka et al does not explicitly teach is
destroying the decryption key after completing playback of the encrypted section.

Stirling et al discloses a method comprising:
destroying the decryption key after completing playback of the encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroying the decryption key after completing playback of the encrypted

Art Unit: 3621

section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

As per claim 17, Peterka et al failed to explicitly disclose the method, further comprising, for each encrypted section:

destroying decrypted data content at the customer processing platform after completing playback of the encrypted section.

Stirling et al discloses a method comprising destroying decrypted data content at the customer processing platform after completing playback of the encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

As per claim 18, Peterka et al discloses the method, wherein the communications medium is the public Internet (fig. 1).

As per claim 19, Peterka et al further discloses the method, wherein, for each encrypted section, the encryption key is the same as the decryption key (0080; 0082; 0117).

As per claim 22, Peterka et al further discloses the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform (0038; 0097; 0114; 0124).

As per claim 23, Peterka et al further discloses the method, wherein receiving each decryption key comprises receiving a transmission value that is determined based on the decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section: recovering the decryption key from the transmission value (0097; 0114; 0124; claim 23).

As per claim 39, Peterka et al further discloses the system, wherein the customer processing platform comprises:

means for requesting the data content to be delivered to the customer processing platform (fig. 1);

means for receiving the plurality of encrypted sections (0080; 0082);

means for receiving, for each encrypted section, the decryption key in respect of the encrypted section (0080; 0082);

means for decrypting and playing back the encrypted section using the decryption key (0080; 0082).

What Peterka et al does not explicitly teach is

Art Unit: 3621

means for destroying the decryption key, after completing playback of the encrypted section.

Stirling et al discloses means for destroying the decryption key, after completing playback of the encrypted section (0080).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Stirling et al in order to ensure that content is only used for the number of times permitted.

5. **Claim 14**, is rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Ginter et al U.S. Patent Application Publication No. 2006/0218651 A1.

As per **claim 14**, Peterka et al discloses the method, further comprising:

delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform; and

delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time (0080; 0082; 0117).

What Peterka et al does not explicitly teach is delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform.

Ginter et al discloses delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform (fig. 28).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Ginter et al in order to encourage wider distribution of content to other participants.

5. **Claims 20 and 43** is rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Stirling et al U.S. patent Application Publication No. 2003/0223583 A1 as applied to claim 16 above, and further in view of Ginter et al U.S. Patent Application Publication No. 2006/0218651 A1.

As per **claims 20 and 43**, both Peterka et al and Stirling et al failed to explicitly disclose the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform.

Ginter et al discloses the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform (fig. 28).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Ginter et al in order to encourage wider distribution of content to other participants.

6. **Claim 34** is rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Negawa U.S. Patent Application Publication No. 2003/0046539 A1.

As per **claim 34**, Peterka et al further discloses a method for controlling use of encrypted data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device (0072; 0123; 0145);

comparing the customer verification information with corresponding stored customer information (0145); and

where the customer verification information is consistent with the stored customer verification information:

Art Unit: 3621

billing a usage charge to an account of the customer (figs. 8 and 9);
transmitting to the customer data content processing device a digital key to
decrypt a current portion of the encrypted data content (fig. 5; 0145); and
for each subsequent portion of the encrypted data:
transmitting to the customer data content processing device a different key to
decrypt the subsequent portion of the encrypted data (fig. 9; 0080; 0082).

What Peterka et al does not explicitly teach is
causing a key for a preceding portion of the encrypted data to be deleted from
the customer data content processing device.

Negawa discloses a method of causing a key for a preceding portion of the
encrypted data to be deleted from the customer data content processing device (0078).

Accordingly it would have been obvious to one of ordinary skill in the art at time
of applicant's invention to modify the method of Peterka et al and incorporate the
method of causing a key for a preceding portion of the encrypted data to be deleted
from the customer data content processing device in view of the teachings of Negawa et
al in order to ensure that content is only used for the number of times permitted.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in
this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 3621

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

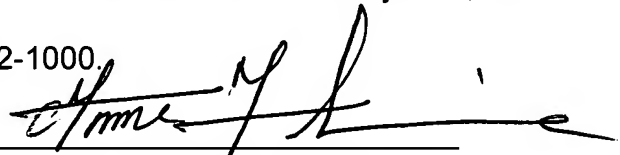
Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is (571) 272-6838. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

Art Unit: 3621


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272 – 6779.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621

Acc
March 14, 2007



ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600